

1 JAMES F. McCABE (CA SBN 104686)
JMcCabe mofo.com
2 BRYAN WILSON (CA SBN 138842)
BWilson mofo.com
3 TERESA N. BURLISON (CA SBN 230854)
TBurlison mofo.com
4 MORRISON & FOERSTER LLP
425 Market Street
5 San Francisco, California 94105-2482
Telephone: 415.268.7000
6 Facsimile: 415.268.7522

7 MARC J. ZWILLINGER (*pro hac vice*)
marc@zwillgen.com
8 ZWILLGEN PLLC
1705 N St. NW
9 Washington, DC 20036
Telephone: (202) 296-3585

10 Attorneys for Defendant
11 APPLE INC., A CALIFORNIA CORPORATION

12
13 UNITED STATES DISTRICT COURT
14 NORTHERN DISTRICT OF CALIFORNIA
15 SAN JOSE DIVISION
16

17 In Re: iPhone/iPad Application Consumer
18 Privacy Litigation

Case No. 5:11-md-02250-LHK

19 **DEFENDANT APPLE INC.'S**
20 **NOTICE OF MOTION AND**
21 **MOTION TO DISMISS**
22 **PLAINTIFFS' FIRST AMENDED**
23 **CONSOLIDATED CLASS**
24 **ACTION COMPLAINT**
25 **PURSUANT TO RULES 12(B)(1)**
26 **AND 12(B)(6); SUPPORTING**
27 **MEMORANDUM OF POINTS**
28 **AND AUTHORITIES**

Date: March 29, 2012
Time: 1:30 p.m.
Ct rm: 8, 4th Floor
Judge: Honorable Lucy H. Koh

NOTICE OF MOTION AND MOTION TO DISMISS

FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

PLEASE TAKE NOTICE THAT at 1:30 p.m. on March 29, 2012 or as soon thereafter as the matter may be heard by the Court, in the Courtroom of the Honorable Lucy H. Koh, located at the Robert F. Peckham Federal Building, 280 South First Street, Fifth Floor, San Jose, California, Defendant Apple Inc., through its attorneys of record, will, and hereby does, move the Court for an order dismissing Plaintiffs' First Amended Consolidated Class Action Complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) with prejudice.

This Motion is based upon this Notice; the attached Memorandum of Points and Authorities; the Declaration of James F. McCabe and the exhibits thereto; the complete files and records of this action, the arguments of counsel, and such other matters that the Court properly may consider.

TABLE OF CONTENTS

	Page
ISSUES PRESENTED.....	1
INTRODUCTION AND SUMMARY OF ARGUMENT	1
I. LEGAL STANDARDS	3
II. ALLEGATIONS IN THE AMENDED COMPLAINT	4
III. PLAINTIFFS' LACK OF STANDING COMPELS DISMISSAL	6
A. Plaintiffs Have Failed Adequately To Allege Injury	6
1. Plaintiffs' Theory That The Collected Data had Economic Value Should Be Rejected Again.	6
2. Plaintiffs' Cost Theories of Injury Have Already Been Rejected By The Court and Are Not Material.	8
3. Plaintiffs' Addition of Stored Communication Act and Wiretap Act Claims Does Not Create An Injury-In-Fact.	9
B. Plaintiffs Fail to Allege Injury Fairly Traceable to Apple.....	10
IV. PLAINTIFFS' CLAIMS ARE FORECLOSED BY THE AGREEMENTS BETWEEN PLAINTIFFS AND APPLE.	11
A. Plaintiffs' Amended Complaint Incorporates Apple's Terms and Conditions and Privacy Policy By Reference.	11
B. The iTunes Store Terms and Conditions Bar These Claims.....	11
1. Apple's Privacy Policy Specifically Authorizes Collection of Anonymized Signal Data.....	11
C. The App Store Terms and Conditions Specifically Disclaim The Liabilities Plaintiffs Seek To Impose on Apple	12
1. Plaintiffs Have Agreed that Apple Has No Duty to Review or Evaluate Apps	13
2. Apple Is Not Liable for Claims Arising from Use of Third Party Products	13
V. EACH OF PLAINTIFFS' CLAIMS SUFFERS FROM ONE OR MORE CLAIM-SPECIFIC DEFECTS.	14
A. The Complaint Does Not State A Claim Against Apple For Violation Of The Stored Communications Act.	15
1. iPhones Are Not "Facilities" for Purposes of the SCA.....	15
2. Location Data on iPhones Is Not in "Electronic Storage."	16

TABLE OF CONTENTS

(continued)

	Page
3. Apple Is Either the Location Service Provider or the Intended Recipient of the Communication, So The SCA Cannot Apply.	17
4. Plaintiffs Have Not Alleged That Apple Accessed a Facility Without Authorization.	18
B. Claim Eleven Does Not State a Claim Against Apple Because There Is No Aiding and Abetting Liability Under The SCA.	19
C. Plaintiffs Have Not Stated a Claim Against Apple for Violation of The Wiretap Act.	20
1. Apple Did Not Intercept Contents of Communications.	20
2. Apple Cannot “Intercept” Information Intended to be Delivered to Apple.	21
D. Plaintiffs Have Not Stated a Claim Against Apple for Violation of The Computer Fraud and Abuse Act.	22
E. The Amended Complaint Does Not State a Claim For Violation of the California Consumer Legal Remedies Act	25
F. The Complaint Does Not State A Claim For Violation Of California’s Unfair Competition Law	26
1. Plaintiffs Fail To Allege Facts Establishing Their Standing To Bring a UCL Claim.	26
2. Plaintiffs Fail To Allege “Fraudulent” Conduct	27
3. Plaintiffs Fail To Allege “Unfair” Conduct By Apple.	28
4. Plaintiffs Fail To Allege “Unlawful” Conduct	29
H. The Complaint Does Not State Any Common Law Or California Constitutional Claims	29
1. The Complaint Fails To State A Claim For Negligence	29
2. The Complaint Fails to State a Claim Under the California Constitution, Conversion, Trespass or Common Counts.	30
CONCLUSION.	30

TABLE OF AUTHORITIES**Page(s)****CASES**

<i>Aas v. Super. Ct.</i> , 24 Cal. 4th 627 (2000)	30
<i>Am. Online, Inc. v. Nat'l Health Care Discount, Inc.</i> , 121 F. Supp. 2d 1255 (N.D. Iowa 2000).....	25
<i>Applied Equip. Corp. v. Litton Saudi Arabia Ltd.</i> , 7 Cal. 4th 503 (1994)	30
<i>Ashcroft v. Iqbal</i> , 129 S. Ct. 1937 (2009).....	3
<i>Bailey v. Bailey</i> , Case No. 07-11672, 2008 WL 324156 (E.D. Mich. Feb. 6, 2008).....	16
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	3, 20, 23
<i>Berryman v. Merit Prop. Mgmt., Inc.</i> , 152 Cal. App. 4th 1544 (2007)	29
<i>Brockey v. Moore</i> , 107 Cal. App. 4th 86 (2003)	29
<i>Buller v. Sutter Health</i> , 160 Cal. App. 4th 981 (2008)	28
<i>Camacho v. Auto. Club of S. Cal.</i> , 142 Cal. App. 4th 1394 (2006)	28
<i>Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.</i> , 20 Cal. 4th 163 (1999)	28
<i>Creative Computing v. Getloaded.com LLC</i> , 386 F.3d 930 (9th Cir. 2004)	24
<i>Crowley v. CyberSource Corp.</i> , 166 F. Supp. 2d 1263 (N.D. Cal. 2001)	18, 22
<i>Czech v. Wall St. on Demand, Inc.</i> , 674 F. Supp. 2d 1102 (D. Minn. 2009).....	24
<i>Davis v. FEC</i> , 554 U.S. 724 (2008).....	3

1	<i>Del Vecchio v. Amazon.com Inc.,</i>	
2	No. C11-366-RSL, 2011 U.S. Dist. LEXIS 138314 (W.D. Wash. Dec. 1, 2011)	7, 9, 24
3	<i>Duarte v. Zachariah,</i>	
4	22 Cal. App. 4th 1652 (1994)	30
5	<i>Durell v. Sharp Healthcare,</i>	
6	183 Cal. App. 4th 1350 (2010)	27
7	<i>Fraley v. Facebook, Inc.,</i>	
8	Case No. 11-CV-01726-LHK, 2011 U.S. Dist. LEXIS 145195 (N.D. Cal. Dec. 16, 2011).....	8
9	<i>Fraser v. Nationwide Mut. Ins. Co.,</i>	
10	135 F. Supp. 2d 623 (E.D. Pa. 2001),	
11	<i>aff'd in part, vacated in part on other grounds,</i> 352 F.3d 107 (3rd Cir. 2003)	16
12	<i>Freeman v. DirecTV, Inc.,</i>	
13	457 F.3d 1001 (9th Cir. 2006)	19
14	<i>Friends of the Earth, Inc. v. Laidlaw Envt'l Servs. (TOC), Inc.,</i>	
15	528 U.S. 167 (2000).....	3
16	<i>Garback v. Lossing,</i>	
17	No. 09-CV-12407, 2010 WL 3733971 (E.D. Mich. Sept. 20, 2010).....	19
18	<i>Genevive LaCourt v. Specific Media,</i>	
19	No. SACV-10-1256-GW, 2011 U.S. Dist. LEXIS 50543 (C.D. Cal. Apr. 28, 2011)	7, 8, 9
20	<i>Hilderman v. Enea TekSci, Inc.,</i>	
21	551 F. Supp. 2d 1183 (S.D. Cal. 2008).....	16
22	<i>In re Actimmune Mktg. Litig.,</i>	
23	No. C 08-02376, 2009 WL 3740648 (N.D. Cal. Nov. 06, 2009).....	29
24	<i>In re Am. Online, Inc., Version 5.0 Software Litig.,</i>	
25	168 F. Supp. 2d 1359 (S.D. Fla. 2001)	23
26	<i>In re Apple & ATTM Antitrust Litig.,</i>	
27	No. C 07-05152, 2010 U.S. Dist. LEXIS 98270 (N.D. Cal. July 8, 2010).....	23
28	<i>In re Doubleclick, Inc., Privacy Litig.,</i>	
	154 F. Supp. 2d 497 (S.D.N.Y. 2001).....	7, 17
	<i>In re Easysaver Rewards Litig.,</i>	
	737 F. Supp. 2d 1159 (S.D. Cal. 2010).....	22
	<i>In re Facebook Privacy Litig.,</i>	
	791 F. Supp. 2d 705 (N.D. Cal. 2011)	26

1	<i>In re JetBlue Airways Corp., Privacy Litig.,</i>	
2	379 F. Supp. 2d 299 (E.D.N.Y. 2005)	7
3	<i>In re Tobacco II Cases,</i>	
4	46 Cal. 4th 298 (2009)	27, 29
5	<i>In re Toys R Us, Inc. Privacy Litig.,</i>	
6	MDL No. M-00-1381 MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001)	16
7	<i>In re VistaPrint Corp. Mktg. & Sales Practice Litig.,</i>	
8	No. 4:08-MD-1994, 2009 WL 2884727 (S.D. Tex. Aug. 31, 2009)	22
9	<i>Jones v. Global Info. Grp., Inc.,</i>	
10	No. 3:06-00246-JDM, 2009 WL 799745 (W.D. Ky. Mar. 25, 2009)	19
11	<i>Kearns v. Ford Motor Co.,</i>	
12	567 F.3d 1120 (9th Cir. 2009)	4, 27
13	<i>Khoury v. Maly's of Cal., Inc.,</i>	
14	14 Cal. App. 4th 612 (1993)	29
15	<i>Ladd v. Cnty. of San Mateo,</i>	
16	12 Cal. 4th 913 (1996)	29
17	<i>Lopez v. Smith,</i>	
18	203 F.3d 1122 (9th Cir. 2000)	3
19	<i>Low v. LinkedIn Corp.,</i>	
20	No. 11-CV-01468-LHK, U.S. Dist. LEXIS 130840 (N.D. Cal. Nov. 11, 2011)	7
21	<i>Meyer v. Sprint Spectrum L.P.,</i>	
22	45 Cal. 4th 634 (2009)	25
23	<i>Northstar Fin. Advisors, Inc. v. Schwab Investments,</i>	
24	781 F. Supp. 2d 926 (N.D. Cal. 2011)	14
25	<i>Rosen v. State Farm Gen. Ins. Co.,</i>	
26	30 Cal. 4th 1070 (2003)	30
27	<i>Rubio v. Capital One Bank,</i>	
28	613 F.3d 1195 (9th Cir. 2010)	11
	<i>Sams v. Yahoo!, Inc.,</i>	
	No. CV-10-5897-JF(HRL), 2011 WL 1884633 (N.D. Cal. May 18, 2011)	21
	<i>Schauer v. Mandarin Gems of Cal., Inc.,</i>	
	125 Cal. App. 4th 949 (2005)	26
	<i>Steve Jackson Games, Inc. v. United States Secret Serv.,</i>	
	36 F.3d 457 (5th Cir. 1994)	16

1	<i>Theofel v. Farey-Jones,</i>	
2	359 F.3d 1066 (9th Cir. 2004)	16
3	<i>Tietsworth v. Sears, Roebuck & Co.,</i>	
4	No. 5:09-CV-00288 JF (HRL), 2009 U.S. Dist. LEXIS 98532 (N.D. Cal. Oct. 13, 2009)	27
5	<i>U.S. v. Reed,</i>	
6	575 F.3d 900 (9th Cir. 2009)	21
7	<i>United States v. Forrester,</i>	
8	512 F.3d 500 (9th Cir. 2008)	21
9	<i>United States v. Smith,</i>	
10	155 F.3d 1051 (9th Cir. 1998)	18
11	<i>United States v. Steiger,</i>	
12	318 F.3d 1039 (11th Cir. 2003)	15, 16
13	<i>Vess v. Ciba-Geigy Corp. USA,</i>	
14	317 F.3d 1097 (2003)	27
15	<i>Whiteside v. Tenet Healthcare Corp.,</i>	
16	101 Cal. App. 4th 693 (2001)	29
17	<i>Wofford v. Apple Inc.,</i>	
18	Case No. 11-CV-0034, 2011 U.S. Dist. LEXIS 129852 (S.D. Cal. Nov. 9, 2011)	25
19	STATUTES	
20	18 U.S.C. § 1030	22, 23
21	18 U.S.C. § 1030(a)	25
22	18 U.S.C. § 1030(a)(4)	23
23	18 U.S.C. § 1030(a)(5)(A)	22
24	18 U.S.C. § 1030(a)(5)(B)	22, 23
25	18 U.S.C. § 1030(a)(5)(C)	22
26	18 U.S.C. § 1030(c)(4)	23
27	18 U.S.C. § 1030(e)(8)	23, 24
28	18 U.S.C. § 1030(e)(11)	23
	18 U.S.C. § 1030(c)(4)(A)	23
	18 U.S.C. § 1030(g)	23, 25

1	18 U.S.C. § 2510.....	20
2	18 U.S.C. § 2510(1)	20
3	18 U.S.C. § 2510(4)	20
4	18 U.S.C. § 2510(8)	20, 21
5	18 U.S.C. § 2510(15)	15
6	18 U.S.C. § 2510(17)	16
7	18 U.S.C. § 2510(17)(B).....	16
8	18 U.S.C. § 2510(18)	20
9	18 U.S.C. § 2511(1)(a).....	21
10	18 U.S.C. § 2511(1)(d)	21
11	18 U.S.C. § 2511(2)(d)	22
12	18 U.S.C. § 2701.....	passim
13	18 U.S.C. § 2701(a)	15, 17, 18
14	18 U.S.C. § 2701(a)(1).....	19
15	18 U.S.C. § 2701(a)(2).....	15
16	18 U.S.C. § 2701(c)	17
17	18 U.S.C. § 2701(c)(1)-(2).....	15, 18
18	18 U.S.C. § 2702.....	10
19	18 U.S.C. § 2707.....	19
20	18 U.S.C. § 2707(a)	19
21	47 U.S.C. § 230(c)(2).....	30
22	Cal. Bus. & Prof. Code § 17200, <i>et seq.</i>	4
23	Cal. Bus. & Prof. Code § 17500, <i>et seq.</i>	29
24	Cal. Civ. Code § 1750.....	4, 25
25	Cal. Civ. Code § 1761(d)	26
26		
27		
28		

OTHER AUTHORITIES

Fed. R. Civ. P. 8(a)(2).....	3
Fed. R. Civ. P. 9(b)	3, 4, 27
Fed. R. Civ. P. 12(b)(1).....	6
Fed. R. Civ. P. 12(b)(6).....	3
Article III of the U.S. Constitution	passim

MEMORANDUM OF POINTS AND AUTHORITIES

ISSUES PRESENTED

1. Whether Plaintiffs' Amended Complaint demonstrates injury-in-fact and causation required to establish Article III standing;
2. Whether Plaintiffs' agreements with Apple bar Plaintiffs' claims;
3. Whether the Amended Complaint fails to state a claim against Apple for which relief can be granted.

INTRODUCTION AND SUMMARY OF ARGUMENT

In dismissing Plaintiffs' first consolidated complaint for lack of Article III standing, this Court found that "Plaintiffs have not identified a concrete harm from the alleged collection and tracking of their personal information" or alleged any "nexus between the alleged harm and Apple's conduct." (Order Granting Defendants' Motion to Dismiss for Lack of Article III Standing with Leave to Amend, Dkt. No. 8 ("Order") at 7, 9.) The Court also detailed extensive "deficiencies with each of Plaintiffs'" claims (*id.* 13), putting Plaintiffs on notice of the need to allege facts showing a plausible injury and other threshold elements. In their Amended Complaint ("AC"), Plaintiffs do not solve their Article III standing problems and largely ignore the Court's directives with regard to the claim-specific deficiencies. The Amended Complaint should be dismissed, this time with prejudice.

Most fundamentally, the Amended Complaint still does not identify a single, concrete injury inflicted on any one of the Plaintiffs here, much less one that is traceable to defendant Apple Inc. ("Apple"). Instead, Plaintiffs continue to rely on the same deficient theories of harm contained in their prior complaint (*i.e.* that Plaintiffs "lost and have not been compensated for the value" of their data and/or the alleged collection of data "consumed portions" of the "memory on their devices") (AC ¶ 72) – theories the Court has soundly rejected. Glaringly absent in their 359-paragraph Amended Complaint is *any* allegation that a single named Plaintiff actually experienced one of these theoretical harms or any concrete injury due to storing or transmitting their anonymous information. And Plaintiffs still cannot point to a single person whose device was actually impaired due to the alleged consumption of storage space or other resources.

Recognizing the lack of actual harm, Plaintiffs seek to persuade the Court that its recycled

1 allegations have an economic component because the data that was allegedly sent to Apple or the
 2 Mobile Industry Defendants had inherent value that the Plaintiffs were entitled to exploit. But a survey
 3 of consumer attitudes is not a proxy for individualized harm. *See* AC ¶ 72(o). And the claim that the
 4 Plaintiffs would have paid less for an iPhone had they known of its true nature is simply an attempt to
 5 recast Plaintiffs' prior allegations of diminished value.¹

6 Plaintiffs' attempt to manufacture an injury-in-fact by adding claims under the Wiretap Act,
 7 Stored Communications Act, and California Constitution that they contend do not require a specific
 8 showing of injury likewise fails. These claims do not provide standing because Plaintiffs do not – and
 9 cannot – allege any of the basic elements required for an invasion of any right under these statutes. For
 10 example, under the SCA and the Wiretap Act, no “communications facilities” were accessed without
 11 authorization, no communications in “electronic storage” were obtained, and no “contents of
 12 communications” were intercepted. Likewise, under the California Constitution, no “legally protected
 13 previous interest” or “serious invasion” of such an interest has been pled.

14 With regard to the causation requirement for Article III standing (which is not impacted by
 15 Plaintiffs' “statutory right” arguments), Plaintiffs again fail to provide “specific allegations with respect
 16 to the causal connection between the exact harm alleged (whatever it is) and each Defendant's conduct
 17 or role in that harm.” (Order at 9.) Plaintiffs' allegations still fail to trace any injury related to the
 18 behavior of over 500,000 applications to Apple's conduct.²

19 Also independently fatal to Plaintiffs' causes of action are Apple's agreements with its
 20 customers, which bar Plaintiffs' claims entirely. Ignoring this Court's requirement that “Plaintiffs must
 21 explain why Apple should be held responsible for privacy violations despite Apple's apparent privacy
 22 agreements with customers, including Plaintiffs” (*id.* at 11), Plaintiffs have made no effort whatsoever to
 23 do so. Apple's agreements with its customers (upon which Plaintiffs continue to rely in the Amended
 24 Complaint) negate Plaintiffs' claims and expressly authorize the conduct complained about here.

25
 26 ¹ The speciousness of Plaintiffs' theory is confirmed by the fact that Plaintiff Lalo bought a new
 iPhone (and does not allege that he paid less than full price) notwithstanding that he was fully aware of
 the allegations in his own complaint. (AC ¶ 36.)

27 ² At the time of the first motion to dismiss, there were over 425,000 apps in the App Store. The
 28 complaint alleges that there are “several hundred thousand Apps in the App Store.” (AC ¶ 89.)

1 Finally, Plaintiffs have ignored the Court's analysis of the numerous claim-specific deficiencies
 2 of the prior complaint, and fail to allege the most basic facts or elements required to plead a viable
 3 claim. Plaintiffs have had ample opportunity to plead a basis for standing or legally sufficient claims
 4 and have been unable to do so. Accordingly, the Amended Complaint should be dismissed with
 5 prejudice.

6 I. LEGAL STANDARDS

7 To establish standing under Article III of the U.S. Constitution, a plaintiff "must show that (1) it
 8 has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not
 9 conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant;
 10 and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable
 11 decision." *Friends of the Earth, Inc. v. Laidlaw Envt'l Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000).
 12 A plaintiff must demonstrate standing for each claim he seeks to press and for each form of relief that is
 13 sought. *See Davis v. FEC*, 554 U.S. 724, 734 (2008).

14 Under Fed. R. Civ. P. 12(b)(6), a court should dismiss a complaint where the plaintiff is unable
 15 to articulate "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v.*
 16 *Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the pleaded factual content
 17 allows the court to draw the reasonable inference that the defendant is liable for the misconduct
 18 alleged." *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009) (citing *Twombly*, 550 U.S. at 556). A court
 19 must consider only the factual allegations of the complaint, not its legal conclusions nor the bare
 20 recitation of the elements of a claim, in determining whether the plaintiff has made a plain statement of
 21 the grounds of her entitlement to relief. *See Fed. R. Civ. P. 8(a)(2); Twombly*, 550 U.S. at 555; *Iqbal*,
 22 129 S. Ct. at 1949. The court must then consider whether the alleged facts state a "plausible," rather
 23 than a merely "possible" claim. *See Iqbal*, 129 S. Ct. at 1950; *Twombly*, 550 U.S. at 555. Where, as
 24 here, there is no plausible claim under the statutes alleged and amendment is futile, the court should
 25 dismiss without leave to amend. *See, e.g., Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (leave to
 26 amend need not be allowed where amendment would be futile).

27 When allegations sound in fraud, Fed. R. Civ. P. 9(b) requires plaintiffs to plead the "who, what,
 28 when, where and how" of the alleged misconduct, including particular misrepresentations on which they

1 supposedly relied. *See Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125-26 (9th Cir. 2009). Plaintiffs’
 2 claims under the Consumer Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.* (“CLRA”) and the
 3 Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* (“UCL”) are subject to the Rule 9(b)
 4 pleading standard. *See Kearns*, 567 F.3d at 1125-26.

5 **II. ALLEGATIONS IN THE AMENDED COMPLAINT**

6 Fundamentally, Plaintiffs’ complaint adds nothing of substance not already presented,
 7 unsuccessfully, in their earlier pleadings. Yet again, Plaintiffs’ claims against Apple boil down to two
 8 core theories – each of which this Court previously rejected.

9 Plaintiffs continue to allege that Apple is liable for app developers’ transmission of supposedly
 10 “personal” data from their iPhones to the Mobile Industry Defendants for advertising or analytics
 11 purposes.³ Specifically, Plaintiffs purport to assert a series of claims based on the fact that they
 12 “downloaded and used numerous free Apps from the App Store,” which they contend resulted in “the
 13 collection of personal information and information about their devices” by the Mobile Industry
 14 Defendants – not Apple. (AC ¶ 45(a).) The Plaintiffs purport to assert these claims on behalf of a
 15 putative class of all U.S. residents who have “purchased iPhones and downloaded free Apps from the
 16 App Store on a mobile device that runs Apple’s iOS, from December 1, 2008” to the present.
 17 (AC ¶ 203.) (Although Plaintiffs refer to this class as the “iDevice Class,” the claims asserted on behalf
 18 of this putative class relate mainly to the use of certain free apps they downloaded from the App Store).

19 Because these allegations are addressed in detail in the Mobile Industry Defendant’s brief in
 20 support of their Motion to Dismiss, Apple does not repeat that discussion here. Critically, however,
 21 Plaintiffs still have not offered anything to change the Court’s prior finding that “there is no allegation
 22 that Apple misappropriated data . . . Plaintiffs’ only allegation is that Apple ‘designed a platform in
 23 which Mobile Industry Defendants and absent app developers could possibly engage in harmful acts...’”
 24 (Order at 9.) (citations omitted.)

25 As for the claims exclusively made against Apple, Plaintiffs still seek to hold Apple liable for the

26 ³ *See, e.g.*, AC ¶¶ 245-46 (alleging Apple is liable for Mobile Industry Defendants’ acquisition of
 27 personal information); *id.* ¶ 252 (alleging duty to protect users from allegedly harmful actions of Mobile
 28 Industry Defendants).

1 presence of certain cell tower/WiFi data on users' own iPhones.⁴ Plaintiffs now also allege that Apple
 2 can use these files to "track" the physical location of users over extended periods of time.⁵ Rather than
 3 files that contain personal data about the Plaintiffs themselves, however, these files are alleged to
 4 contain raw data about cell towers and WiFi hotspots that are encountered by Plaintiffs' iPhones.
 5 Indeed, Plaintiffs' allegations are that Apple is developing a database containing information about the
 6 physical *location of publicly visible cell towers and Wi-Fi hotspots* across the United States. (AC
 7 ¶ 137.) (emphasis added.) Plaintiffs do not allege that the cell towers and Wi-Fi hotspots data personally
 8 identified them.

9 Plaintiffs assert three claims based on the storage of cell tower/WiFi data,⁶ but only on behalf of
 10 the putative "Geolocation Class," persons who turned off "Location Services" on their iPhones before
 11 April 27, 2011. (*Id.* ¶ 204.) Plaintiffs allege that the iOS 4 operating system stored information about
 12 "Plaintiffs' precise geographic location" in a file on the iPhone (*id.* ¶ 115) and periodically transmitted
 13 that information to Apple. (*Id.* ¶ 116.) Plaintiffs also allege that because iOS 4 did not encrypt the file
 14 containing this cell tower/WiFi data, the data could be accessible to an unauthorized person who "may
 15 have access to a computer used to back-up one's iPhone." (*Id.* ¶ 152.) By this, they mean that if
 16 hackers break into their home computers, there is a possibility that they could access the file after it is
 17 backed-up. This is a wildly theoretical harm, not one that actually occurred. It also is the very type of
 18 information the Privacy Policy states Apple may collect. As the Privacy Policy states, "location
 19 information is collected anonymously in a form that does not personally identify you." (Declaration of
 20 James F. McCabe in Support of Defendant Apple Inc.'s Motion to Dismiss First Consolidated Class
 21 Action Complaint, Dkt. No. 143, ("McCabe Decl.") Ex. G at 5.) The Privacy Policy also makes clear
 22 that Apple considers location data to be "non-personal information" which Apple may collect and use to

23
 24 ⁴ See AC ¶ 255(a), (c) (Apple failed to "fulfill its commitments" by storing unencrypted location
 25 history information on iPhones); *id.* ¶ 264 (Apple violated the CFAA by transmitting code that caused
 26 users' iPhones to maintain, synchronize and retain unencrypted location history files); *id.* ¶ 308(a)
 27 (Apple trespassed by using memory); and *id.* ¶ 287 (incorporating alleged violation of CFAA).

28 ⁵ AC ¶ 107(a) (geolocation cache allegedly available to Apps); *id.* ¶¶ 137-38 (Apple is developing a
 database of the location of cell towers and wireless networks); *id.* ¶¶ 143-44 ("Apple . . . is able to
 approximate the exact location of thousands, if not millions, of United States citizens . . .").

⁶ See First Claim for Relief, Stored Communications Act; Second Claim for Relief, Electronic
 Communications Privacy Act; Third Claim for Relief, California Right to Privacy.

1 improve products, services and advertising.” (*Id.* at 3.)

2 Moreover, Plaintiffs Gupta and Rodimer make no allegation that any third parties obtained
3 access to cell tower/WiFi data on their iPhones, or that they suffered any harm from its creation. And
4 there is no allegation that Apple attempted to use, much less exploit, the cell tower/WiFi data to track
5 movements of any class member. Instead, the Amended Complaint engages in vague and unsupported
6 speculation about the implausible, theoretical harms that supposedly *could* occur *if* various unauthorized
7 parties somehow accessed this cell tower/WiFi data – without alleging that any of this harm actually
8 happened. (*Id.* ¶152 (data could be accessible to an unauthorized person who “may have access to a
9 computer used to back-up one’s iPhone.”); *id.* ¶ 144 (“Apple – or anyone else with access to this
10 geolocation data – is able to approximate the exact location of thousands, if not millions, of United
11 States citizens...”)).

12 **III. PLAINTIFFS’ LACK OF STANDING COMPELS DISMISSAL**

13 The Amended Complaint suffers from the same deficiencies as the prior complaint and should be
14 dismissed under Fed. R. Civ. P. 12(b)(1) because Plaintiffs lack standing. This Court previously held
15 that Plaintiffs had failed “to allege injury in fact to *themselves*” or to “identif[y] a concrete harm from
16 the alleged collection and tracking of their personal information sufficient to create injury in fact” for
17 purposes of Article III standing. (Order at 6-7.) Moreover, the Court found that Plaintiffs had failed to
18 allege any injury that was fairly traceable to *Apple* and specifically directed that “any amended
19 complaint must provide specific allegations with respect to the causal connection between the exact
20 harm alleged (whatever it is) and each Defendants’ conduct or role in that harm.” (*Id.* at 9.) Plaintiffs’
21 Amended Complaint does not address these threshold deficiencies and still cannot point to a single
22 example of harm caused by Apple (or anyone).

23 **A. Plaintiffs Have Failed Adequately to Allege Injury.**

24 Plaintiffs’ theories of injury can be placed in two broad categories – those related to personal
25 data and those related to the supposed use of iOS Device resources. Each is discussed below.

26 **1. Plaintiffs’ Theory That The Collected Data had Economic Value** 27 **Should Be Rejected Again.**

28 The Court soundly rejected Plaintiffs’ argument that “personal” data has economic value that is

1 somehow “lost” or diminished when shared for advertising or analytics purposes. (Order at 17-18).
 2 Relying on *Genevive LaCourt v. Specific Media*, No. SACV-10-1256-GW, 2011 U.S. Dist. LEXIS
 3 50543 (C.D. Cal. Apr. 28, 2011), the Court held:

4 Plaintiffs have not yet articulated a “coherent and factually supported theory” of injury.
 5 Plaintiffs have stated general allegations about the Mobile Industry Defendants, the market
 6 for Apps, and similar abstract concepts (e.g., lost opportunity costs, value-for-value
 exchanges), but Plaintiffs have not identified an actual injury to themselves sufficient for
 Article III standing.

7 (Order at *18.)

8 Since this Court’s Order, several other decisions have followed its ruling and the reasoning in
 9 *Specific Media*. See *Del Vecchio v. Amazon.com Inc.*, No. C11-366-RSL, 2011 U.S. Dist. LEXIS
 10 138314, at *10-11 (W.D. Wash. Dec. 1, 2011) (rejecting claims that Amazon’s harvesting of user data
 11 without consent deprived them of “the opportunity to exchange their valuable information” for lack of
 12 Article III standing, finding this theory to be “entirely speculative” because, “[w]hile it may be
 13 theoretically possible that Plaintiffs’ information could lose value as a result of its collection and use by
 14 Defendant, Plaintiffs do not plead any facts from which the Court can reasonably infer that such
 15 devaluation occurred in this case.”); *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, U.S. Dist. LEXIS
 16 130840, at *4-5, 11 (N.D. Cal. Nov. 11, 2011) (allegations that LinkedIn’s technology allowed third
 17 parties to track online browsing history “without the compensation to which [plaintiff] was due” were
 18 “too abstract and hypothetical to support Article III standing.”). These recent cases follow a line of
 19 earlier cases holding that unauthorized collection of personal information does not create an economic
 20 loss. See *In re JetBlue Airways Corp., Privacy Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005)
 21 (disclosed passenger data had no compensable value); *In re Doubleclick, Inc., Privacy Litig.*, 154 F.
 22 Supp. 2d 497, 525 (S.D.N.Y. 2001) (unauthorized collection of personal information by third party does
 23 not create “economic loss”).

24 The Amended Complaint fails for the same reason. Plaintiffs still do not point to a single
 25 specific detail showing “what harm (if any) resulted from the access or tracking of [Plaintiffs’] personal
 26 information.” (Order at 6.) And, Plaintiffs’ enhanced allegations about location data are a red herring
 27 because such data – by Plaintiffs’ own admission – is about the location of cell site towers and Wi-Fi
 28 hotspots and not personally tied to Plaintiffs. Rather than add facts explaining how (or whether) any

Plaintiff was harmed, the complaint continues to rely on academic papers and abstract concepts, without alleging any facts specific to the named Plaintiffs or the information that supposedly was collected by the Mobile Industry Defendants. (*See, e.g.*, AC ¶ 72(o) referencing “Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach.”.) It is the same “abstract concept[s] such as ‘lost opportunity costs’ and ‘value-for-value exchanges’” that this Court and other courts repeatedly have held to be insufficient to establish Article III standing. *See Specific Media*, 2011 U.S. Dist. LEXIS 50543 (finding Plaintiffs’ reference to academic articles about willingness to disclose data insufficient for standing); *Fraley v. Facebook, Inc.*, Case No. 11-CV-01726-LHK, 2011 U.S. Dist. LEXIS 145195 (N.D. Cal. Dec. 16, 2011) (collecting and distinguishing conjectural harm cases from actual harm cases). Plaintiffs’ “information collection” theories of harm fare no better this time around.

2. Plaintiffs’ Cost Theories of Injury Have Already Been Rejected By The Court and Are Not Material.

Despite this Court’s directive, Plaintiffs again fail to allege that the collection of their “information”, or cell tower and Wi-Fi hot spot data, had any actual impact on them or their devices – a fact confirmed by Plaintiff Lalo’s purchase of a second iPhone *after* filing this case against Apple. *See* section IV(B)(1), *supra*. Plaintiffs’ vague allegations of “undisclosed transmittal fees,” “loss of battery power” and “reductions in storage space” – which are not tied to any specific Plaintiff or device – rehash the theories of their prior complaint and still fail to allege that any specific Plaintiff experienced concrete injury.⁷ Plaintiffs do not allege that the presence of cell tower/WiFi data on their devices had *any* concrete impact on the utility of their devices or them. No Plaintiff alleges, for example, that she ran out of storage capacity or was prevented from downloading an app due to the consumption of storage resources on her iPhone. Under Plaintiffs’ own calculations, the location file utilizes a trivial amount of the iPhone’s storage capacity (at most ¼ of 1%). This alone is dispositive. Plaintiffs also make no allegation supporting their alleged “right” to have the storage capacity of their device unencumbered by the operation of iOS 4. In other words, Plaintiffs never allege Apple promised them an unencumbered 16GB or 32GB of storage capacity or that Apple would not use that capacity for operating system files.

⁷ Compare AC ¶¶ 76, 79-84, 87, with Compl. ¶¶ 170-71.

1 Like any operating system and software, iOS 4 and pre-installed applications occupy storage space on
 2 users' devices. Accordingly, consuming storage space for iOS files cannot be an injury-in-fact that
 3 supports standing.

4 As in *Specific Media*, “[i]f Plaintiffs are suggesting that their computers’ performance was
 5 compromised in some other way . . . then they need to allege facts showing this is true.” 2011 U.S. Dist.
 6 LEXIS 50543, at *13; *see also Amazon.com*, 2011 U.S. Dist. LEXIS 138314, at *11 (dismissing claims
 7 for lack of standing where “not one of the Plaintiffs alleges that he or she discerned any difference
 8 whatsoever in the performance of his or her computer while visiting Defendant’s site, let alone any
 9 diminution from which the Court could plausibly infer the necessary damages.”); and Order at 9 (citing
 10 *Birdsong*, 590 F.3d at 961) (“‘conjectural’ or speculative allegations about the risk of harm do not
 11 suffice for purposes of Article III standing”). Here, Plaintiffs do not cite a single, concrete example or
 12 allege that their iPhones’ performance or the use of their iPhones has been affected in any way due to
 13 Apple’s alleged conduct or otherwise.

14 Likewise, Plaintiffs’ conclusory assertion that they somehow paid a “wrongful premium” for
 15 their iPhones based on “undisclosed costs” imposed on iPhone users (*See* AC ¶ 80) goes nowhere.
 16 Plaintiffs do not point to a single, specific misrepresentation Apple allegedly made at the time of
 17 purchase that materially influenced their decision making. Given that their prior allegations of
 18 diminished capacity and impaired value were insufficient to confer standing, Plaintiffs cannot now
 19 circumvent that holding by merely adding the allegation that they would not have purchased the device
 20 had they known about either the presence of cell tower/WiFi data on their iPhones or the ability of
 21 various applications to obtain data about their device usage.

22 **3. Plaintiffs’ Addition of Stored Communication Act and Wiretap** 23 **Act Claims Does Not Create An Injury-In-Fact.**

24 Plaintiffs have added claims under the Wiretap Act, Stored Communications Act and California
 25 Constitution, in the hope that asserting these claims, without more, will avoid the need to allege any
 26 actual injury. *See* Order at 8 (“Plaintiffs, in the instant case, do not allege a violation of [the Wiretap
 27 Act or] an analogous statute which does not require a showing of injury.”). But Plaintiffs cannot satisfy
 28 the “injury” requirement under Article III merely by adding statutory or constitutional claims to their

pleading where they do not even *allege* the basic elements of these claims or that they, “themselves,” have experienced the invasion of any right created by these statutes. As discussed below, the Wiretap Act creates a limited statutory right not to have the contents of communications intercepted by a third party. Here, Plaintiffs do not allege that the “content” of any of their communications was “intercepted” by Apple (which it alleges *created* the data that was “communicated”), or any other credible claim that a right under that statute was violated. *See* section V(C), *infra*. Similarly, Plaintiffs do not allege an SCA claim because they do not plead that Apple accessed any “communications facilit[y]” without authorization, or that it obtained any of Plaintiffs’ communications in “electronic storage” from such a facility. Mere reference to these statutes plainly is not enough to show injury where the conduct alleged is not within the scope of the law. *See* section V(A), (B), *infra*.

B. Plaintiffs Fail To Allege Injury Fairly Traceable To Apple.

Separately, Plaintiffs still fail to allege a nexus between any alleged harm and Apple’s conduct, or to show that their alleged injuries are “fairly traceable” to Apple, as required to satisfy Article III standing requirements. (Order at 9.) Despite the Court’s Order putting Plaintiffs “on notice . . . that any amended complaint must provide specific allegations” as to “each Defendant’s conduct or role” in “the exact harm alleged,” Plaintiffs have not added a *single factual detail* explaining how Apple caused any one of them identifiable harm. (*Id.*) Although the Amended Complaint adds details about what information was allegedly transferred by five apps⁸ to certain Mobile Industry Defendants (AC ¶¶ 58-68), it adds nothing to suggest that any Plaintiff was injured by *Apple* due to this alleged conduct. Instead, Plaintiffs continue to allege that Apple somehow is responsible for the activities of third-party apps and their vendors due to its operation of the App Store, and due to the manner in which it “designed its iPhone’s iOS 4 to collect and send geolocation data . . . to Apple’s servers.” (*Id.* ¶ 138; *see also id.* ¶¶ 4, 143-44, 150.) But the Court previously rejected each of these platform-based theories, correctly finding that they failed to demonstrate any concrete harm caused by Apple:⁹

⁸ Of course, Plaintiffs are not seeking to hold Apple liable for the practices of only the few applications described in the Amended Complaint, but for the behavior of all 500,000 apps in the App store.

⁹ *Compare* Compl. ¶¶ 6, 58, 63, 68, 71-73, 117, 125, 194, *with* AC ¶¶ 88-99, 168-69, 264, 334.

Plaintiffs' only allegation is that Apple "designed" a platform in which Mobile Industry Defendants and absent app developers could possibly engage in harmful acts . . . or that Apple's platform caused "users" iDevices to be able to maintain, synchronize, and retain detailed, unencrypted location history files.... These "conjectural" or speculative allegations about the risk of harm do not suffice for purposes of Article III Standing.

(Order at 9.) As with their last pleading, the Amended Complaint does not contain a single fact establishing that any Plaintiff suffered an identifiable harm that is fairly traceable to Apple's operation of the App Store or iOS 4.

IV. PLAINTIFFS' CLAIMS ARE FORECLOSED BY THE AGREEMENTS BETWEEN PLAINTIFFS AND APPLE.

Even if Plaintiffs could somehow demonstrate Article III standing – and they cannot – Plaintiffs' agreements with Apple bar the claims asserted in the Amended Complaint. In its Order, the Court directed Plaintiffs to explain in any amended complaint "why Apple should be held responsible for privacy violations despite Apple's apparent privacy agreements with customers, including Plaintiffs." (Order at 11.) Plaintiffs have not responded to this directive.

A. Plaintiffs' Amended Complaint Incorporates Apple's Terms and Conditions and Privacy Policy By Reference.

As the Court found in its Order and at the hearing on September 8, 2011, this Court may consider Plaintiffs' agreements with Apple under the incorporation by reference doctrine. (*See* Order at 10; *Rubio v. Capital One Bank*, 613 F.3d 1195, 1199 (9th Cir. 2010).) Here, the Amended Complaint again cites the Terms and Conditions for the iTunes Store (AC ¶¶ 77-78, 139, 315), which includes Apple's Privacy Policy (*See id.* ¶¶ 78, 315); therefore the Court may consider the contents of these agreements.

B. The iTunes Store Terms and Conditions Bar These Claims.

Before any Plaintiff could download an app onto her iPhone or use an app (including free apps), she was required to create an iTunes account and agree to the iTunes Store Terms and Conditions and Privacy Policy. As demonstrated below, the plain terms of these agreements foreclose their claims based on the collection of location information or on third party conduct.

1. Apple's Privacy Policy Specifically Authorizes Collection of Anonymized Signal Data.

Apple's Privacy Policy is found in Section D of the iTunes Store Terms and Conditions and as a

standalone document elsewhere on the Apple website. Its express terms negate two different conclusory allegations in the Amended Complaint: first, that Apple’s collection of location data from iPhones is unauthorized and second, that such data is “personal” (or “personally identifying”).

Specifically, the iTunes’ Privacy Policy affords Apple a broad right to collect, use and transfer both device identifier and location-related information:

[Apple] may collect, use, transfer, and disclose non-personal information for any purpose. The following are some *examples* of non-personal information that we collect and how we may use it:

We may collect information such as occupation, language, zip code, area code, *unique device identifier, location*, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.

(McCabe Decl., Ex. G at 1-2.) (emphasis added.) While Plaintiffs repeatedly contend that they are aggrieved by the alleged transfer of device UDIDs through their use of apps (AC ¶¶ 102-106); *Plaintiffs have specifically consented to such transfers*: as a condition of obtaining apps through the App Store, Plaintiffs agreed that Apple could “collect, use, transfer *and disclose* . . . unique device identifier [UDID] and location.” (McCabe Decl., Ex. G at 1-2.)

Likewise, as Plaintiffs concede, the Privacy Policy explicitly provides for Apple’s collection, from iOS Devices, of location data, and makes clear that the data does not identify the user:

To provide location-based services on Apple products, *Apple* and our partners and licensees *may collect, use, and share precise location data*, including the real-time geographic location of your Apple computer or device. *This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services.*

(*Id.* at 4.) (emphasis added.) The Privacy Policy also confirms that the cell tower/WiFi data is not “personal” information, which includes only “data that can be used *to uniquely identify* or contact a single *person*.” (*Id.* at 1.) (emphasis added.) Indeed, Apple specifically identifies “location” as “non-personal information” – i.e. “data in a form that does not permit direct association with any specific individual.” (*Id.* at 2.) Plaintiffs’ own agreements thus preclude them from recharacterizing the location data cache as “personal” information.

C. The App Store Terms and Conditions Specifically Disclaim The Liabilities Plaintiffs Seek To Impose on Apple.

As in their prior complaint, Plaintiffs seek to hold Apple liable because third-party app

1 developers allegedly (a) used apps distributed through the App Store to collect information from iPhones
 2 or iPads; (b) transferred collected information to the Mobile Industry Defendants; and (c) did so without
 3 or in excess of the user's consent. (*See, e.g.*, AC ¶¶ 246, 251-53, 316, 321, 336-341.) Yet, the Terms
 4 and Conditions applicable to users "download[] and use" of these apps specifically provide that Apple
 5 has no liability arising from their use of third-party Apps.

6 **1. Plaintiffs Have Agreed That Apple Has No Duty to Review or**
 7 **Evaluate Apps.**

8 The App Store Terms and Conditions (Section C of the iTunes Terms and Conditions, McCabe
 9 Decl., Ex. F at 8) set the terms that govern the use of the App Store. While Plaintiffs continue to allege
 10 that Apple is obligated to police the behavior of more than 85,000 App Developers and other third
 11 parties, the App Store Terms and Conditions specifically disclaim any such obligation:

12 Apple has the right, but not the obligation, to monitor any materials . . . available on the App
 13 and Book Services . . .

14 Certain content, App and Book Products, and services available via the App and Book
 15 Services may include materials from third parties. ***You agree that Apple is not responsible***
 16 ***for examining or evaluating the content*** or accuracy and ***Apple does not warrant and will***
not have any liability or responsibility for any third-party materials or websites, or for any
 other materials, ***products*** or services ***of third parties.***

17 (*Id.* at 10.) (emphasis added.) Contrary to Plaintiffs' claims, their contracts with Apple expressly
 18 disclaim any duty to review and police App content. (*See, e.g.*, Comp. ¶¶ 125, 131, 132, 133.) Apple's
 19 alleged decision to remove some apps from the App Store, but not others, does not waive this provision
 20 and oblige Apple to review all apps in the App Store. *See* McCabe Decl., Ex. F at 12 ("Apple's failure
 21 to enforce any right or provisions in his [sic] Agreement will not constitute a waiver...").

22 **2. Apple Is Not Liable for Claims Arising from Use of Third Party Products.**

23 Because Apple has no obligation to review third party apps in the first place, Apple does not
 24 warrant and has no liability for claims, like those here, arising from the operation of those apps. Every
 25 user of the App Store specifically has agreed:

26 **THAT YOUR USE OF . . . THE APP AND BOOK SERVICES IS AT YOUR SOLE**
 27 **RISK. THE APP AND BOOK SERVICES AND ALL PRODUCTS AND APP AND**
 28 **BOOK SERVICES DELIVERED TO YOU THROUGH THE APP AND BOOK**
SERVICES ARE (EXCEPT AS EXPRESSLY STATED BY APPLE) PROVIDED "AS
IS" AND "AS AVAILABLE" FOR YOUR USE, WITHOUT WARRANTIES OF ANY

KIND, EITHER EXPRESS OR IMPLIED, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY [OR] FITNESS FOR A PARTICULAR PURPOSE . . .

(*Id.* at 12 (caps in original; emphasis added).) Plaintiffs thus may not now imply a guarantee from Apple that third party apps meet Apple's Developer Guidelines or any other standard.

Likewise, Plaintiffs have agreed that the developer of the app, not Apple, is solely responsible for any claims arising from their use of an app:

The Application Provider of each Third-Party Product is solely responsible for that Third-Party Product, the content therein, any warranties to the extent that such warranties have not been disclaimed, ***and any claims that you or any other party may have relating to that Third-Party Product.***

(*Id.*) (emphasis added.) This is reinforced by Plaintiffs' detailed waiver of such claims:

IN NO CASE SHALL APPLE, ITS DIRECTORS, OFFICERS, EMPLOYEES, AFFILIATES, AGENTS, CONTRACTORS, PRINCIPALS OR LICENSORS **BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING FROM YOUR USE OF ANY OF THE APP AND BOOKS SERVICES OR FOR ANY OTHER CLAIM** RELATED IN ANY WAY TO YOUR USE OF THE APP AND BOOK SERVICES

Id. at 12 (caps in original; emphasis added). In other words, to take one example, Plaintiff Rodimer has agreed that if he believes he has a claim over the data handling practices of the Bible App, he can look only to its developer, not to Apple, for relief. Plaintiffs' agreements with Apple thus unambiguously defeat any claim they may have arising from their use of third party apps.¹⁰

V. EACH OF PLAINTIFFS' CLAIMS SUFFERS FROM ONE OR MORE CLAIM-SPECIFIC DEFECTS.

Even if the Court were to conclude that Plaintiffs have (i) somehow alleged an injury-in-fact traceable to Apple (they have not), and (ii) identified a claim not foreclosed by the Plaintiffs' agreements with Apple (they have not), each of the claims in the Amended Complaint nonetheless should be dismissed with prejudice in light of the additional claim-specific defects discussed below.

¹⁰ Plaintiffs' new conclusory assertion that they are third-party beneficiaries of contracts between Apple and app developers should not be credited. There is no forced mutuality to third party beneficiary status. "If a contract does not clearly evince the intent to benefit a third party, that party is not a beneficiary of the contract." *Northstar Fin. Advisors, Inc. v. Schwab Investments*, 781 F. Supp. 2d 926, 943 (N.D. Cal. 2011). Plaintiffs have identified no language "clearly evinc[ing] the intent" to make them third party beneficiaries of any agreement between Apple and App Developers. *Id.*

A. The Complaint Does Not State A Claim Against Apple for Violation of the Stored Communications Act.

Plaintiffs' new allegations under the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 *et seq.*) fare no better than their rehashed causes of action and fail to state a claim. Section 2701 prohibits "(1) intentionally access[ing] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[ing] an authorization to access that facility; and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage in such system." § 2701(a).

To state a claim for a violation of § 2701, Plaintiffs must identify a "facility through which an electronic communication service is provided," describe the electronic communications that were in "electronic storage" in that facility, and plead facts that would support the finding of an unauthorized "access." The Amended Complaint fails to meet these requirements for four reasons: (1) an iOS Device is not a "facility through which an electronic communication service is provided;" (2) the cell tower/WiFi data is not in "electronic storage"; (3) the claim is barred by the exceptions contained in 18 U.S.C. § 2701(c)(1)-(2) because Apple either provides the location services at issue, or is the intended recipient of the location data; and (4) Plaintiffs do not allege that Apple accessed plaintiffs iPhones through unauthorized log-ins, only that the iPhones communicated with Apple's servers. As a result, liability under the SCA is barred as a matter of law.

1. iPhones Are Not "Facilities" for Purposes of the SCA.

To violate § 2701, a defendant must access a "facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(2). In turn, an electronic communication service is "any service which provides to *users* thereof the ability to send and receive wire or electronic communications." 18 U.S.C. § 2510(15) (emphasis added). The computer systems of an email provider (like Google), a bulletin board system (like Craigslist), or an ISP (like Verizon) are all examples of facilities that provide electronic communications services to multiple users. *See United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) ("the SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system BBS.") By contrast, an individual's computer, laptop, or mobile device – which provides only its owner and not

third parties with the ability to send and receive messages – is plainly not a facility under the SCA. *See id.* (holding a laptop computer is not a facility). Here, Plaintiffs’ allege that an iPhone was the affected “facility” (AC ¶¶ 224-25), which is contrary to existing precedent and makes clear the SCA does not apply.¹¹

2. Location Data on iPhones Is Not in “Electronic Storage.”

Information that is stored on a user’s iPhone cannot be information in “electronic storage” for purposes of the SCA. The SCA is designed to prevent third parties from accessing emails and other communications while they are stored temporarily awaiting delivery (or any backup of such communications). Under Section 2701, “electronic storage” is not synonymous with “stored in electronic form,” as Plaintiffs suggest. Instead, electronic storage is defined as “(a) any temporary, intermediate storage of a wire or electronic communication *incidental to the electronic transmission thereof*; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” § 2510(17) (emphasis added). Plaintiffs’ attempt to categorize the location data as information in “electronic storage” simply does not meet the statutory definition.

Instead, the SCA’s definition of electronic storage applies to “messages not yet delivered to their intended recipient”¹² or messages in backup storage.¹³ *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004); *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 461-62 (5th Cir. 1994). Accordingly, to state a claim under the SCA, Plaintiffs must plead facts supporting a finding that location data was stored temporarily in an electronic communication service facility on an incidental basis pending the delivery of this data to the recipient. Here, however, the Plaintiffs plead the exact

¹¹ *See Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1204 (S.D. Cal. 2008) (“It is questionable whether the laptop computer qualifies as a ‘facility through which an electronic service is provided.’”). *See also Bailey v. Bailey*, Case No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (SCA “protection does not extend to emails and messages stored only on Plaintiff’s personal computer.”).

¹² *See Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001) (messages in post-transmission storage were outside scope of § 2701), *aff’d in part, vacated in part on other grounds*, 352 F.3d 107 (3rd Cir. 2003); *In re Toys R Us, Inc. Privacy Litig.*, MDL No. M-00-1381 MMC, 2001 U.S. Dist. LEXIS 16947, at *10-11 (N.D. Cal. Oct. 9, 2001) (same).

¹³ Plaintiffs have not pled that the location cache is stored for backup protection. Indeed, they cite only the first half of the definition of electronic storage, and the second half of the definition is inapplicable in any event. *See* AC ¶ 221, *citing* 18 U.S.C. § 2510(17)(A) not § 2510(17)(B).

opposite: “in the [] folder on a user’s iDevice, Apple maintains an unencrypted log of the user’s movements ... for up to a one-year period.” (AC ¶ 107(a).) Plaintiffs thus do not allege that the information is in storage for a limited time incidental to its transmission. Nothing about the alleged storage of this file on an iPhone is akin to intermediate storage of email by ISPs waiting for users to download messages from their servers.

The court in *In re Doubleclick, Inc., Privacy Litigation*, dismissed a SCA claim for the same reason, finding that the identification numbers for browser cookies the defendants installed on the Plaintiffs’ computers were not in “electronic storage.” 154 F. Supp. 2d at 511-12. Interpreting subsection (a), the court clarified that the SCA “only protects electronic communications stored ‘for a limited time’ in the ‘middle’ of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it.” *Id.* at 512 (“Congress’ intent was to protect communications held in interim storage by electronic communication service providers.”) The SCA thus does not protect cookies because they “remain on plaintiffs’ computers for a virtually indefinite time period.” *Id.* (internal citations omitted).

Plaintiffs cannot allege that the location-related file is in “electronic storage,” because the storage they describe is neither temporary nor incidental to its transmission; thus, for this additional reason, they cannot state a § 2701 claim against Apple.

3. Apple Is Either The Location Service Provider or The Intended Recipient of The Communication, So The SCA Cannot Apply.

Even if Plaintiffs had alleged that Apple accessed a communication in “electronic storage” in a “communications facility,” this conduct would fall under specific SCA exceptions for service providers or intended parties to certain communications, providing that § 2701(a) does not apply to “conduct authorized: (1) by the person or entity providing a wire or electronic communications service; (2) by a user of that service with respect to a communication of or intended for that user.” 18 U.S.C. § 2701(c); *see also In Re Doubleclick*, 154 F. Supp. 2d at 514-15 (finding cookie identification numbers, if in storage, are “of or intended for” Doubleclick and exempt under (c)(2)). Here, Plaintiffs claim that Apple itself caused a log of geolocation data to be generated and stored (AC ¶¶ 107(a), 114); and that Apple designed the iPhone to collect and send this data to Apple servers. (*Id.* ¶ 138.) The Amended

Complaint does not describe a transmission between third parties that Apple improperly accessed – it describes instead Apple’s use of the Plaintiffs’ iPhones to store certain data which it later sent back to itself, allegedly without the user’s authorization.¹⁴ This is not a § 2701 violation.¹⁵ Although the Amended Complaint does not specifically identify the “facility,” the parties to the “communication,” or who is providing the “service,” it either describes Apple’s activities in the course of providing location services on the user’s device, or communications the user’s device sent to Apple. Regardless of how the Amended Complaint is read – neither is actionable, as § 2701(c)(1)-(2) expressly excludes such activities from the SCA.

4. Plaintiffs Have Not Alleged That Apple Accessed a Facility Without Authorization.

Finally, Plaintiffs have failed to allege another critical element of an SCA claim – that Apple “accessed” their iPhones “without authorization” in order to obtain the location data.¹⁶ To violate § 2701, a defendant must have accessed the “facility” in question “without authorization.” 18 U.S.C. § 2701(a). Even if there were a “facility” in this case, there still would be no unauthorized “access” to it. The Ninth Circuit has held that the word “access” should be given its plain meaning, namely “to get at” or “gain access to.” *United States v. Smith*, 155 F.3d 1051, 1058 (9th Cir. 1998). Applying this meaning, the court in *Crowley* dismissed the SCA claim because Crowley’s information was sent to Amazon: “[Amazon] did not access the information as that term is used in the [SCA].” *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1272-73 (N.D. Cal. 2001).

Here, Plaintiffs allege that Apple violated the SCA “by intentionally accessing its consumers’ communications without authorization . . . by collecting temporarily stored location data from Plaintiff Gupta and the Geolocation Class’s iPhones after Locations Services was turned ‘Off.’” (AC ¶ 224.) As a threshold matter, these allegations misstate the requirements of Section 2701, which prohibits “accessing *a facility* without authorization” (not unauthorized access to a *communication*). Moreover, the only concrete allegations all indicate Apple received transmissions that were

¹⁴ But this conduct was authorized under the Privacy Policy, *see* section IV(B)(1), *infra*.

¹⁵ And for reasons described in section V(D), *infra* it also cannot be the basis for a CFAA claim.

¹⁶ This flaw also bars their CFAA claims. *See* section V(D), *infra*.

“transmitted”¹⁷ or “sent”¹⁸ directly from the iPhones to Apple’s servers, much in the way an email or text message might be sent. This is not the same as logging in, without authorization, to a communication facility. But even if it were considered “access,” such access was fully authorized for the reasons described in section VI(B), *supra*. Thus, dismissal is warranted.

B. Claim Eleven Does Not State A Claim Against Apple Because There Is No Aiding And Abetting Liability Under The SCA.

Plaintiffs’ additional claim for relief under the SCA (claim 11) alleges that all of the Defendants have violated § 2701(a)(1) by “intentionally accessing . . . consumers’ communications without authorization and obtaining and/or altering authorized access to a wire or electronic communication while in electronic storage by collecting temporarily stored location data from the iDevice Class’ iPhones as set forth in paragraphs 58 through 64, above.” (AC ¶ 347.) The sole support for this claim pertains to activities by the Mobile Industry Defendants who allegedly acquired stored location data through use of Plaintiffs’ apps. (*Id.* ¶¶ 58-64.) This claim fails for the reasons set forth in the Mobile Industry Defendants’ Motion. In any event, particularly in the absence of any allegations as to Apple’s role, Apple cannot be liable for the actions of others because there is no aiding and abetting liability under the SCA. Instead, the statute extends civil liability only to “the person or entity . . . which engaged in [the] violation.” 18 U.S.C. § 2707(a); *Freeman v. DirecTV, Inc.*, 457 F.3d 1001 (9th Cir. 2006) (declining to expand civil liability under §§ 2702 and 2707 of the SCA to aiders, abettors, or other conspirators).¹⁹ Because Plaintiffs never claim that *Apple* used any apps to collect users’ data, Apple cannot be held liable for a violation of the SCA on this basis (or otherwise), and the claim should be dismissed with prejudice.

¹⁷ See AC ¶¶ 30, 46-47, 142, 145, 204 (alleging ‘transmission’ of data).

¹⁸ See AC ¶¶ 138, 150 (alleging “sending” of data).

¹⁹ See also *Garback v. Lossing*, No. 09-CV-12407, 2010 WL 3733971, at *6 n.6 (E.D. Mich. Sept. 20, 2010) (§§ 2701 and 2707 do not include secondary liability); *Jones v. Global Info. Grp., Inc.*, No. 3:06-00246-JDM, 2009 WL 799745, at *3 (W.D. Ky. Mar. 25, 2009) (“since Congress did not criminalize the actions of aiding and abetting violations of 18 U.S.C. § 2701 as part of that statute, and § 2707 authorizes awards of damages to private parties but does not mention aiders and abettors or other secondary actors, this court will not infer secondary civil liability pursuant to 18 U.S.C. § 2707”).

C. Plaintiffs Have Not Stated A Claim Against Apple for Violation Of The Wiretap Act.

As with their SCA claims, Plaintiffs' own pleading defeats Plaintiffs Gupta's and Rodimer's attempt to state a claim under the Wiretap Act (18 U.S.C. §§ 2510 *et seq.*). Here, the Wiretap Act claim is based on the alleged interception of Gupta's and Rodimer's "wire and/or electronic communications." (AC ¶ 230.) Although the Amended Complaint never specifies what communications Apple supposedly intercepted (or identifies the parties to any communication), it suggests that the basis for the interception claim is the same as for the SCA claim – Apple's alleged programming of the iPhones to save and report location data. Recording location data, however, cannot support a claim under the Wiretap Act because (1) it is not the content of any communication, and (2) Apple is an intended recipient of the communication, not a third party.

1. Apple Did Not Intercept Contents of Communications.

Plaintiffs' claim under the Wiretap Act fails because the Amended Complaint does not properly allege that Apple intercepted the "contents" of any communications. The Wiretap Act defines "intercept" as "the aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added).²⁰ To sustain a claim for interception of electronic communications, Plaintiffs must plead facts to support the claim that an intercept occurred; they cannot simply recite the statutory language. *Twombly*, 550 U.S. at 555. Here, the Amended Complaint does not allege the interception of "contents." The Wiretap Act defines the "contents" of a communication narrowly as "any information concerning the substance, purport, or meaning of that communication." § 2510(8). Although Plaintiffs allege that the term "contents" includes information about the "identity of the parties to such communication" and therefore imply that it covers the location data at issue here – it does not. The phrase "identity of parties to such communication" contained in paragraph 229 of the amended

²⁰ Here, no wire communications are at issue. A wire communication is defined as "any *aural* transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." 18 U.S.C. § 2510(1) (emphasis added). And an aural transfer is a communication where a human voice can be heard. § 2510(18). The complaint never refers to interception of phone calls and therefore fails to allege the interception of a "wire communication."

complaint is not in the text of the Wiretap Act. Indeed, Congress *struck* this precise language from 18 U.S.C. § 2510(8) in 1986. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, § 101(a)(5) (1986) (striking “identity of the parties to such communication or the existence” from 18 U.S.C. § 2510(8)). Not only did Plaintiffs misstate the definition of “contents” in the complaint by relying on a 25-year old repealed version of the law, but they did so using the exact same language as the plaintiff in *Sams v. Yahoo!, Inc.*, No. CV-10-5897-JF(HRL), 2011 WL 1884633 at * 7 (N.D. Cal. May 18, 2011). In *Sams*, this Court dismissed a claim against Yahoo! for disclosure of “contents” of a communication that relied on the same mischaracterization. *See id.*

Information about the identities of parties to a communication and other call data *is not content*. In *U.S. v. Reed*, 575 F.3d 900 (9th Cir. 2009), the Ninth Circuit considered whether data about a telephone call, such as the call’s time of origination and the length, constituted a “communication” for purposes of the Wiretap Act’s sealing provisions. *Id.* at 914. The court made clear that “content” is limited to information the user intended to communicate, like the words spoken in a phone call. *Reed*, 575 F.3d at 916. Accordingly, the court found that automatically generated data about the phone call – like the call’s source and duration – “contains no ‘information concerning the substance, purport, or meaning of [the] communication.’” *Id.* (quoting 18 U.S.C. § 2510(8)); *see also United States v. Forrester*, 512 F.3d 500, 503 (9th Cir. 2008) (holding IP addresses and other “addressing information,” including the email addresses of the parties to the communication are not content). Because Plaintiffs fail to allege that Apple intercepted the “content” of any of Plaintiffs’ communications, the Wiretap Act claim must be dismissed.²¹

2. Apple Cannot “Intercept” Information Intended To Be Delivered To Apple.

Plaintiffs also cannot state a claim because the Amended Complaint specifically alleges that Apple was a party to the location data that supposedly was “intercepted.” (*See* AC ¶ 142 (“Apple designed iOS 4 to access and transmit location data from the mobile device to Apple’s servers....”).) The Wiretap Act states in pertinent part that it is not “unlawful . . . for a person not acting under color of

²¹ Because Plaintiffs’ claim for illegal interception under § 2511(1)(a) fails, their claims for use or disclosure of allegedly illegally intercepted data under § 2511(1)(d) must also fail. AC ¶ 231.

law to intercept a wire, oral, or electronic communication, *where such person is a party to the communication.*” 18 U.S.C. § 2511(2)(d) (emphasis added). *See Crowley*, 166 F. Supp. 2d at 1269 (“Amazon merely received the information transferred to it by Crowley, an act without which there would be no transfer. Amazon acted as no more than the second party to a communication.”).²² Here, Plaintiffs’ own allegations – that Apple designed software that would report location data back to its servers – defeats any claim that Apple was a third-party who intercepted communications between others.

D. Plaintiffs Have Not Stated A Claim Against Apple for Violation Of The Computer Fraud and Abuse Act.

Following dismissal of their earlier CFAA claim, Plaintiffs responded by alleging three theories under the CFAA. None, however, is sufficient to survive dismissal.²³ Specifically, Plaintiffs allege claims under the following provisions:

- 18 U.S.C. § 1030(a)(5)(A)²⁴ for knowingly causing the “transmission of a command to be downloaded to Plaintiffs’ iDevices.” (AC ¶ 269.)
- 18 U.S.C. § 1030(a)(5)(B) for “intentionally accessing” Plaintiffs’ “iDevices without authorization, and as a result ... recklessly causing damage to Plaintiffs’ and Class Members’ iDevices by impairing the integrity of data and/or system and/or information.” (*Id.* ¶ 270.)
- 18 U.S.C. § 1030(a)(5)(C) for accessing Plaintiffs’ and Class Members’ protected computers without authorization and causing damage and loss. (*Id.* ¶ 271.)

Claims under Subsections (B) & (C) fail because each requires Apple to have “accessed” Plaintiffs’ devices “without authorization,” which Apple has not done. And all three require Plaintiffs to demonstrate more than \$5,000 in damages related to the unauthorized access. Plaintiffs’ theory of harm is insufficient to overcome this hurdle.

Apple did not access a device without authorization. To state a claim under §§ 1030(a)(5)(B) & (C), a plaintiff must allege that the defendant accessed a protected computer “without authorization.”

²² *See also In re Easysaver Rewards Litig.*, 737 F. Supp. 2d 1159, 1184 (S.D. Cal. 2010) (same); *In re VistaPrint Corp. Mktg. & Sales Practice Litig.*, No. 4:08-MD-1994, 2009 WL 2884727, at *28 (S.D. Tex. Aug. 31, 2009) (dismissing Wiretap Act claim under § 2511(2)(d) exception where defendants “were parties to the communications, receiving the information that Plaintiffs transmitted to them”).

²³ This section addresses Count Six. Count Seven also purports to allege claims against all Defendants, but the substance is directed toward the Mobile Industry Defendants, not Apple.

²⁴ Plaintiffs invoke 18 U.S.C. § 1030(a)(5)(A)(i-iii) but there are no such subsections in § 1030 as presently in force. Apple assumes Plaintiffs intended to allege claims under the revised statute.

1 But, the complaint only makes formulaic recitations of the elements by stating that “Apple violated 18
2 U.S.C.[§] 1030 by intentionally accessing Plaintiffs’ ... iDevices without authorization or by exceeding
3 authorization.”²⁵ (AC ¶ 262.) Such “a formulaic recitation of the elements of a cause of action will not
4 do.” *Twombly*, 550 U.S. at 555.

5 Moreover, other allegations in the Amended Complaint make clear that Apple did not access any
6 iOS Devices without authorization. The Amended Complaint alleges that Apple “caused the
7 transmission to users’ iDevices, either by native installation or iOS upgrade, of code that caused users’
8 iDevices to maintain, synchronize, and retain detailed, unencrypted location history files.” (AC ¶ 264.)
9 But these methods of installing software are nothing more than the “voluntary installation” this Court
10 previously found deficient. (Order 11) (citing *In re Apple & ATTM Antitrust Litig.*, No. C 07-05152,
11 2010 U.S. Dist. LEXIS 98270, at *26 (N.D. Cal. July 8, 2010).) Native installations are performed
12 before Apple sells the phone, and thus by definition cannot be unauthorized. Likewise, users must
13 choose to install iOS upgrades, and the amended complaint therefore does not (and cannot) allege that
14 these updates were performed without the users’ consent. (*See* AC ¶ 94 (“When a user installs Apple’s
15 updates to the iDevice operating system...”)); *In re Am. Online, Inc., Version 5.0 Software Litig.*, 168 F.
16 Supp. 2d 1359, 1370 (S.D. Fla. 2001) (AOL did not access a computer without authorization when users
17 voluntarily downloaded and installed its software).

18 Second, Plaintiffs again have failed to meet the damages threshold. In order to state a civil claim
19 under the CFAA, Plaintiffs must allege they suffered “damage or loss by reason of a violation of” the
20 CFAA *and* that they suffered at least \$5,000 in economic damage in a one-year period as a result of
21 Defendants’ actions. *See* 18 U.S.C. § 1030(g) & (c)(4)(A)(i)(I).²⁶

22 Plaintiffs’ theory of harm cannot support a CFAA damage claim. (AC at ¶¶ 118-122.) No court
23

24 ²⁵ Neither Subsection (B) or (C) provides liability for exceeding authorized access. *Compare* 18
25 U.S.C. § 1030(a)(4). Plaintiffs do not attempt to state a claim under Subsection (a)(4), nor could they,
because they have not alleged that a Plaintiff’s location data is a “thing of value.”

26 ²⁶ The CFAA defines “loss” as “any reasonable cost to any victim, including the cost of responding
27 to an offense, conducting a damage assessment, and restoring the data, program, system, or information
28 to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages
incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). “Damage” is defined “as
impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C.
§ 1030(e)(8) (emphasis added).

has held that merely occupying space in computer memory or storage constitutes “impairment” damage under 18 U.S.C. § 1030(e)(8). In *Czech v. Wall St. on Demand, Inc.*, 674 F. Supp. 2d 1102 (D. Minn. 2009), for example, the plaintiff alleged that receiving unwanted text messages caused damage because they “deplete or exhaust a cell phone’s limited RAM or ROM, thereby causing its other operations or functions to slow or lock up completely” and “deplete or consume the phone’s hard drive memory storage capacity.” *Id.* at 1115. The court rejected this theory of damage based on mere consumption of storage – finding it *so implausible* that it chose to ignore such allegations and construe the pleadings to refer *only* to receipt of messages that would cause a slowdown in service. *Id.* at 1117. As the *Czech* court observed, the “problem with such a theory is that that it would extend ‘damage’ under the CFAA to include the receipt of any unwanted electronic communication” or indeed any form of data, including software updates, “under any circumstance.” *Id.* Such a reading would render the damage requirement superfluous. Thus, other courts have also found that the use of a computer’s resources can be sufficient damage *only* where it results in actual impairment of a user’s ability to use the service *in addition to* the loss of storage capacity.²⁷ Additionally, even if there were some “damage” here, which there is not, Plaintiffs have not alleged plausibly that they suffered, even collectively, at least \$5,000 in economic damage in a one-year period (due to a single act or otherwise). Plaintiffs’ argument also defies common sense. *Apple* designs its iOS, and the size of the operating system is within its discretion. Each iOS iteration uses a different amount of storage on a device – and a user has no control over the file size. Under Plaintiffs’ theory, any unwanted feature that takes up space on a user’s device causes damage merely by its presence. (AC ¶ 121.) Contrary to the complaint’s bald assertion of a “superior” right in hard drive space, the CFAA does not make the use of storage space by an operating system into a criminal act or the basis for civil liability.

Plaintiffs’ theory also fails because any reduction in storage capacity was not caused by the alleged transmission of data – but by Apple’s design choices. Plaintiffs must prove that they suffered

²⁷ See *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004); see also *Del Vecchio v. Amazon.com Inc.*, No. C11-366-RSL, 2011 U.S. Dist. LEXIS 138314, at *11 (W.D. Wash. Nov. 30, 2011) (“[N]ot one of the plaintiffs allege that he or she discerned any difference whatsoever in the performance of his or her computer while visiting Defendant’s site, let alone any diminution from which the Court can plausibly infer the necessary damages.”).

1 “damage or loss *by reason of*” the particular violation of § 1030(a). *Am. Online, Inc. v. Nat’l Health*
 2 *Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1275-76 (N.D. Iowa 2000). Plaintiffs’ theory would hold
 3 Apple liable *only* because of a design choice to store cell tower/WiFi data on the iPhone, rather than its
 4 own servers. If Apple had chosen server-side storage, there would have been no effect on storage space,
 5 and thus, no “damage.” But as this Court held in its prior order, under 18 U.S.C. § 1030(g), “negligent
 6 software design cannot serve as a basis for a CFAA claim.” (Order at 16.) But the “single act of harm”
 7 that is now alleged here (as the basis for aggregating damages) *is* Apple’s software design. Accordingly,
 8 Plaintiffs CFAA claim should be dismissed with prejudice.

9 **E. The Amended Complaint Does Not State A Claim For Violation Of the**
 10 **California Consumer Legal Remedies Act.**

11 The Consumer Legal Remedies Act (“CLRA”), California Civil Code § 1750 *et seq.*, provides
 12 protection to consumers who *sustain damage* as the result of the purchase or lease of a good or service.
 13 Here, for the reasons discussed in section III(A) above, Plaintiffs did not suffer injury or damage, as
 14 required for a CLRA violation. *See, e.g., Meyer v. Sprint Spectrum L.P.*, 45 Cal. 4th 634, 638 (2009) (“a
 15 plaintiff has no standing to sue under the CLRA without some allegation that he or she has been
 16 damaged by an alleged unlawful practice”). This alone requires dismissal of Plaintiffs’ CLRA claim.
 17 *See* Order at 14 (dismissing Plaintiff’s CLRA claim because “Plaintiffs have not alleged ‘any damage’
 18 as a result Defendants’ alleged actions”).

19 Moreover, as this Court held, the CLRA does not apply to software (such as free apps, operating
 20 systems, or iOS upgrades), which is not a “good” or “service” under the CLRA. (Order at 14, citing
 21 *Ferrington v. McAfee*, 2010 U.S. Dist. LEXIS 106600, at *52-58; *accord Wofford v. Apple Inc.*, Case
 22 No. 11-CV-0034, 2011 U.S. Dist. LEXIS 129852, at *6 (S.D. Cal. Nov. 9, 2011) (“California law does
 23 not support [the] contention that software is a tangible good or service of the purposes of the CLRA.”)).
 24 Indeed, *Wofford* specifically held that allegations about iOS4 were not actionable for this reason. Like
 25 their earlier pleading, Plaintiffs’ “allegations against Apple [are] about software, i.e., the iOS operating
 26 system on iDevices.” *Wofford*, 204 U.S. Dist. LEXIS 129852 at * 6. Because “software is neither a
 27 ‘good’ nor a ‘service’ within the meaning of the CLRA,” their CLRA claims again must be dismissed.
 28 *Id.*

Finally, a CLRA violation may only be alleged by a “[c]onsumer,” defined as “an individual who seeks or acquires, *by purchase or lease*, any goods or services for personal, family, or household purposes.” Cal. Civ. Code §1761(d) (emphasis added); *see In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011); *Schauer v. Mandarin Gems of Cal., Inc.*, 125 Cal. App. 4th 949, 960 (2005) (non-purchaser of a ring was not “consumer” who could maintain CLRA claim). But Plaintiffs did not “purchase or lease” the free apps on which they base their claims. Accordingly, such persons are not “consumers” within the meaning of the CLRA. The CLRA claim should be dismissed with prejudice.

F. The Complaint Does Not State A Claim For Violation Of California’s Unfair Competition Law.

1. Plaintiffs Fail To Allege Facts Establishing Their Standing To Bring a UCL Claim.

As this Court previously recognized, to assert a UCL claim, “a private plaintiff needs to have ‘suffered injury in fact and ... lost money or property as a result of the unfair competition.’” (Order at 19) (*citing Rubio v. Capital One Bank*, 613 F.3d 1195, 1203 (9th Cir. 2010)); *see also Birdsong*, 590 F.3d at 960 (“Plaintiffs must show . . . that they suffered *a distinct and palpable injury* as a result of the alleged unlawful or unfair conduct.”).) This Court concluded that Plaintiffs had not “adequately alleged *any* injury, let alone an injury of ‘lost money or property.’” (Order at 20.)

The Amended Complaint does not cure this fatal flaw. As the Court’s Order recognized, “Numerous courts have held that a plaintiff’s ‘personal information’ does not constitute money or property under the UCL.” (*Id.* at 19-20.) Plaintiffs’ primary allegations still relate to the alleged transmission of allegedly “personal information” to the Mobile Industry Defendants by third-party App developers, or the alleged collection of location information by Apple, and thus do not satisfy the UCL injury requirement. Similarly, Plaintiffs’ conclusory theories of injury based on the alleged consumption of memory or resources on their iPhones do not establish standing under the UCL, since Plaintiffs do not point to any specific property that they “lost” due to the supposed activities complained of here. Plaintiffs’ failure to allege that they “lost money or property” as the result of any unfair conduct by Apple (or otherwise) again requires dismissal of their UCL claims.

2. Plaintiffs Fail To Allege “Fraudulent” Conduct.

The Ninth Circuit has specifically held that Rule 9(b)’s heightened pleading standard applies to

1 fraud-based claims under the UCL, “whether affirmative misrepresentations or omissions.” *Kearns*,
 2 567 F.3d at 1127. Rule 9(b) requires that “a party must state with particularity the circumstances
 3 constituting fraud” or mistake. *Id.* at 1126. Conclusory allegations of fraud are insufficient. *Vess v.*
 4 *Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (2003). “Averments of fraud must be accompanied by
 5 ‘the who, what, when, where, and how’ of the misconduct charged” (*Kearns*, 567 F.3d at 1124), as well
 6 as the circumstances indicating fraudulent conduct (*Vess*, 317 F.3d at 1106). Further, Plaintiffs must set
 7 forth specific allegations establishing that they actually relied on the alleged misrepresentations or
 8 omissions. *In re Tobacco II Cases*, 46 Cal. 4th 298, 326 (2009).

9 Plaintiffs’ amended complaint does not satisfy these requirements. Plaintiffs’ UCL “fraud”
 10 claim offers only the conclusory allegation that “Plaintiffs and members of the Class were deceived by
 11 Apple’s representations” and “reasonably relied on Apple’s representations.” (AC ¶ 339.) That is
 12 precisely the type of conclusory allegation that does not satisfy Rule 9(b). The individual named
 13 Plaintiffs do not describe with particularity any allegedly fraudulent statement that they saw, or when or
 14 where they saw it. That failure is fatal to their UCL claim. *Kearns*, 567 F.3d at 1126.

15 Perhaps most fundamentally, Plaintiffs do not allege facts demonstrating that they relied on any
 16 specific misrepresentation or omission. Actual reliance by the named plaintiffs is a necessary element of
 17 a UCL claim for fraudulent business practices. *In re Tobacco II Cases*, 46 Cal. 4th at 326. Plaintiffs
 18 must allege specific facts demonstrating that the “alleged misrepresentations: 1) were relied upon by the
 19 named Plaintiffs; 2) were material; 3) influenced the named plaintiffs’ decisions to purchase; and
 20 4) were likely to deceive members of the public.” *Tietzworth v. Sears, Roebuck & Co.*, No. 5:09-CV-
 21 00288 JF (HRL), 2009 U.S. Dist. LEXIS 98532, at *25 (N.D. Cal. Oct. 13, 2009) (citing *Tobacco II*, 46
 22 Cal. 4th at 326-28); *see also Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1363 (2010).
 23 Plaintiffs’ conclusory allegation that the class members reasonably relied on Apple’s representations
 24 does not meet this standard. *In re Tobacco II Cases*, 46 Cal. 4th at 326 (“Reliance is proved by showing
 25 that the defendant’s misrepresentation is an ‘immediate cause’ of the plaintiff’s conduct by showing that
 26 in its absence the plaintiff ‘in all reasonable probability’ would not have engaged in the injury-producing
 27 conduct.”) (quoting *Mirkin v. Wasserman*, 5 Cal. 4th 1082, 1110-11 (1993)). Plaintiffs fail to state a
 28 claim under the fraud prong of the UCL.

3. Plaintiffs Fail To Allege “Unfair” Conduct By Apple.

Plaintiffs also fail to allege “unfair” conduct under the UCL. To state a UCL claim for “unfair” conduct, a plaintiff must allege facts establishing (1) a substantial consumer injury; (2) that the injury is not outweighed by countervailing benefits to consumers; and (3) that the injury is one that consumers could not reasonably have avoided. *See Camacho v. Auto. Club of S. Cal.*, 142 Cal. App. 4th 1394, 1403 (2006). The amended complaint does not satisfy any of these requirements.

First, and as discussed above, Plaintiffs’ inability to provide facts supporting substantial (or any) consumer injury dooms their UCL “unfairness” claim. (AC ¶¶ 331-32.) This Court has already held that Plaintiffs’ primary theory of injury – alleged transfer of personal information – does not constitute a loss of money or property actionable under the UCL. Plaintiffs’ theory respecting storage of location data fares no better. By Plaintiffs’ own calculations, that data occupies a scintilla of device memory and, more importantly, is not alleged to have affected Plaintiffs or their devices in any way. Plaintiffs’ thus fail to allege substantial injury.

Plaintiffs also fail to demonstrate how the iPhones’ numerous benefits and technical advances are outweighed by the ethereal harms Plaintiffs allege. Finally, and most damning, there is no evidence that Plaintiffs were compelled to purchase iPhones or to download Apps. With the wide range of alternatives available to every iDevice Apple makes, Plaintiffs could readily have bought a different device. (AC ¶ 333.)

Plaintiffs seek to salvage their UCL “unfairness” theory by relying on an alternative test. Under that test, for a business practice to be “unfair,” that “unfairness” must be “tethered” to a legislatively declared policy. *Cel-Tech Commc’ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 186-87 (1999); *Buller v. Sutter Health*, 160 Cal. App. 4th 981, 991 (2008). But Plaintiffs have not articulated the requisite “tether” to a statutory policy. The amended complaint makes vague reference to the CLRA, the constitutional right to privacy, and nebulous “California statutes’ recognition of the need for consumers to be information [sic] and equipped to protect their own privacy interests.” (AC ¶ 333.) That is not sufficient; Plaintiffs “identif[y] no particular section of the statutory scheme which was violated and [fail] to describe with any reasonable particularity the facts supporting violation.” *Khoury v. Maly’s of Cal., Inc.*, 14 Cal. App. 4th 612, 619 (1993). Accordingly, Plaintiffs fail to allege an

1 “unfairness” claim under the UCL.

2 **4. Plaintiffs Fail To Allege “Unlawful” Conduct.**

3 As demonstrated previously, the amended complaint also fails to allege a violation of any law,
4 and thus fails to state a claim under the UCL’s “unlawful” prong. *See Berryman v. Merit Prop. Mgmt.,*
5 *Inc.*, 152 Cal. App. 4th 1544, 1554 (2007) (“violation of another law is a predicate for stating a cause of
6 action under the UCL’s unlawful prong.”); *Whiteside v. Tenet Healthcare Corp.*, 101 Cal. App. 4th 693,
7 706 (2001) (same.)²⁸

8 **H. The Complaint Does Not State Any Common Law Or California** 9 **Constitutional Claims.**

10 **1. The Complaint Fails To State A Claim For Negligence.**

11 Plaintiffs’ negligence claim fails because Plaintiffs cannot support their conclusory allegation
12 that Apple somehow had a duty not to collect location data or to prevent apps from sharing their
13 information, and also because they allege no harm. The elements of a cause of action for negligence are
14 well established under California law. They are “(a) a *legal duty* to use due care; (b) a *breach* of such
15 legal duty; [and] (c) the breach as the *proximate or legal cause* of the resulting injury.” *Ladd v. Cnty. of*
16 *San Mateo*, 12 Cal. 4th 913, 917 (1996) (quoting *Evan F. v. Hughson United Methodist Church*, 8 Cal.
17 App. 4th 828, 834 (1992) (italics in original).)

18 Although Plaintiffs claim that Apple owed a duty to Plaintiffs “to protect their personal
19 information and data property . . .” (AC ¶ 249) and a “duty to protect Plaintiffs from the harmful actions
20 that Apple knew would be caused by the use of Apps” (*id.* ¶ 252), Plaintiffs fail to allege any legal basis
21 for such “duties.” In fact, the App Store Terms and Conditions expressly *disclaim* any obligation to
22 review apps offered through the App Store and any liability for any claim related to third party apps,
23
24

25 ²⁸ Plaintiffs assert, without detail, that Apple violated Cal. Bus. & Prof. Code § 17500 *et seq.* (the
26 False Advertising Law or “FAL”). The requirements of a FAL claim, however, are the same as a claim
27 under the fraud prong of the UCL. *In re Tobacco II Cases*, 46 Cal. 4th at 312 n.8; *Brockey v. Moore*,
28 107 Cal. App. 4th 86, 98 (2003); *In re Actimmune Mktg. Litig.*, No. C 08-02376, 2009 WL 3740648, at
*15 (N.D. Cal. Nov. 06, 2009). Accordingly, Plaintiffs’ FAL claim fails for the reasons set forth in
sections IV(F)(1-2) above.

1 which includes any claims as to how apps handle device and customer information.²⁹ Likewise, the
 2 Privacy Policy *permits* Apple to collect location-related information using iPhones, and to send such
 3 information, in anonymized form, to its servers. It is well settled that tort law cannot be used to imply a
 4 duty that has been expressly disclaimed by contract. Likewise, the failure to perform a contractual duty
 5 is never a tort, unless that failure involves an independent legal duty. *See Applied Equip. Corp. v. Litton*
 6 *Saudi Arabia Ltd.*, 7 Cal. 4th 503, 514-15 (1994).

7 In addition, for the reasons addressed in detail in section III(A), Plaintiffs also fail to allege an
 8 “appreciable, non-speculative, present injury,” which is “an essential element of a tort cause of action.”
 9 *Aas v. Super. Ct.*, 24 Cal. 4th 627, 646 (2000) (*superseded by statute on other grounds as stated in*
 10 *Rosen v. State Farm Gen. Ins. Co.*, 30 Cal. 4th 1070, 1079-80 (2003)); *see also Duarte v. Zachariah*, 22
 11 Cal. App. 4th 1652, 1661-62 (1994) (actual damage in “the sense of ‘harm’ is necessary to a cause of
 12 action in negligence; nominal damages are not awarded”). Plaintiffs’ threadbare claim that they
 13 somehow “were harmed as a result of Apple’s breach of its duties, which damage is separate and apart
 14 from any damage to their iPhones themselves” does not suffice to allege a plausible, non-speculative
 15 injury. (AC ¶ 257.) Because Plaintiffs fail to allege the breach of any legal duty or any resulting injury,
 16 the amended complaint fails to state a claim for negligence.

17 **2. The Complaint Fails to State a Claim Under the California** 18 **Constitution, Conversion, Trespass or Common Counts.**

19 Finally, Plaintiffs’ claims for violation of the right of privacy under the California Constitution,
 20 Conversion, Trespass, and Common Counts fail for the reasons stated in the Mobile Industry
 21 Defendants’ motion to dismiss, which are equally applicable to Apple. To avoid unnecessary repetition
 22 of those legal arguments, Apple incorporates them by reference herein.

23 **CONCLUSION**

24 For the foregoing reasons, Apple respectfully requests that the Court dismiss all claims against it,
 25 with prejudice.

26
 27 ²⁹ To the extent the negligence claim relies on Apple’s decision to remove certain apps from the App
 28 Store and not others, this theory of liability would be foreclosed by Section 230 of the Communications
 Decency Act. *See* 47 U.S.C. § 230(c)(2).

1 Dated: January 10, 2012

JAMES F. MCCABE
BRYAN WILSON
TERESA N. BURLISON
MORRISON & FOERSTER LLP

2
3
4 MARC J. ZWILLINGER
ZWILLGEN PLLC

5
6 By: /s/ James F. McCabe
James F. McCabe

7 Attorneys for Defendant
8 APPLE INC., a California Corporation
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28